



## CJIS Vendor Management Program

The CBI Crime Information Management and Identification Units are proud to present the CJIS Vendor Management Program. This program is designed make it easier for vendors to meet CJIS Security Policy standards. By streamlining the fingerprinting process and the audit process where applicable, the CBI anticipates greater options will become available for the use, management and sharing of CJIS data in Colorado.

### How does a business join the CJIS Vendor Management Program?

Businesses providing CJIS services to Colorado Criminal Justice Agencies may contact the CBI Crime Information Management Unit (CIMU), or the CBI Identification Unit to obtain a vendor packet. Carefully review and complete the CBI CJIS Vendor Agreement, and the CBI New Account Application and return the documents to CBI. Please note your business will be responsible for payment of \$39.50 for each employee fingerprint submission and an additional fees for FBI-CJIS subsequent arrest notifications, i.e. "rap-back," when that program is established. CIMU personnel will review fingerprint background check responses and notify the vendor if any employees are ineligible to access CJIS data due to criminal history. Business providing shared services may be offered the opportunity to consolidate audits similarly.

### Getting Started - Steps for CJIS Services Vendors:

1. Request vendor packet from CBI
2. Fill out and return the CJIS Vendor Agreement, Account Application form, and W-9 included.
3. Receive account number (known as a RAF number) from CBI by email. This takes about one week to establish.
4. Submit fingerprints on all staff members supporting CJIS systems using the CBI-provided RAF number. Fingerprints may take about one week to process and authorize staff members.
5. Ensure ongoing compliance with CJIS Security Policy

### How does the CJIS Vendor Management Program help Law Enforcement Agencies?

Once vendor personnel are fingerprinted, Colorado Law Enforcement Agencies will have the ability to search by vendor or by employee information to verify the vendor employee has been fingerprinted in Colorado. Employees determined to be eligible to support CJIS information will be listed so the agency may verify their identity and background. This will eliminate the need for each agency to receive a set of individual fingerprints for each employee of a vendor who supports multiple agencies.

### Steps for Law Enforcement Agencies:

1. Inform vendors of the program
2. Provide vendor packet to vendor
3. Check CCIC to verify fingerprinting and authorization status of vendor personnel.
4. Check CJIS Online for vendor, employees. Add if necessary.

### CJIS Certified?

Because CJIS Compliance is a process that can change as technology and law enforcement's business needs change, participation in this program does not guarantee CJIS certification. However, it demonstrates a working knowledge of CJIS standards and a commitment to maintain these high standards.

## Frequently Asked Questions – CJIS Vendor Management

*There are CJIS vendors who have been working in Colorado with several law enforcement agencies. Do those need to have our personnel re-fingerprinted?*

Yes. In the past, law enforcement agencies have had individuals from private companies fingerprinted under their ORI. In order to make the fingerprint status available to all law enforcement in Colorado, the vendor employees will need to be re-fingerprinted under the CBI-issued RAF.

*Can a law enforcement agency require additional background checks beyond the fingerprint-based background check performed by CBI?*

Yes. The CBI vendor management program ensures the minimum background check required by FBI-CJIS standards is performed. A law enforcement agency may have a more restrictive policy.

*Can a law enforcement agency use a CJIS vendor who has chosen not to participate in the program?*

Yes. However, the agency will need to perform their own fingerprinting of all vendor employees. Additional law enforcement agencies using the same vendor will also need to perform their own fingerprinting.

*Do all employees working for a CJIS vendor need to undergo a fingerprint-based background check?*

No. A CJIS vendor may have other facets of their business which are separate from their CJIS business. However, all vendor employees with responsibilities for configuring systems and networks with direct access to CJI; as well as employees with physical and/or logical access to CJI must also undergo a fingerprint-based background check. This may include the same type of support personnel as are fingerprinted within the law enforcement agency including human resource staff, janitorial staff and others.

*Why would a vendor employee be shown as “Not Authorized”?*

Upon receipt of fingerprints, they are processed by FBI and CBI. New fingerprints will show “not authorized” until the results of the fingerprint check are reviewed by a CBI employee and the criminal history is verified to be free of felony convictions. If a felony conviction, or a felony arrest without a disposition are found, the employee will remain as “not authorized.” An employee with a felony conviction cannot have any access to CJIS information.

*This program is a cooperative effort between the CBI Crime Information Management Unit (CIMU) and the Identification Unit (Ident). Questions may be sent to [CDPS.CBI.CCIC@state.co.us](mailto:CDPS.CBI.CCIC@state.co.us). A dedicated email address for this program is forthcoming.*